The opinion in support of the decision being entered today was *not* written for publication in and is *not* binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Ex parte RAANAN LIEBERMANN

Appeal 2007-0215
Application 09/662,451
Technology Center 1700

Decided: March 16, 2007

Before STUART S. LEVY, LINDA E. HORNER, and ANTON W. FETTING, *Administrative Patent Judges.*

FETTING, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF CASE

This appeal involves claims 1-7, 9-64 and 122[1], the only claims pending in this application. We have jurisdiction over the appeal pursuant to 35 U.S.C. §§ 6 and 134.

We AFFIRM-IN-PART.

---

[1] Claims 8 and 65-121 are cancelled.

The Appellant invented a system to secure personal transactions (Specification 6). An understanding of the invention can be derived from a reading of exemplary claim 1, which is reproduced below.

> 1. A method for carrying out personal transactions comprising:
>
> providing a system for performing said personal transactions;
>
> registering a user of said system;
>
> said registering step comprising said user accessing said system and providing said system with personal information about said user;
>
> said registering step further comprising selecting an identification number for said user;
>
> said registering step further comprising creating a PIN number by selecting a plurality of single digit numbers to act as a first segment of said PIN number; and
>
> said PIN number creating step further comprising selecting at least two digits for a security segment to be incorporated into said PIN number wherein an alarm signal is sent when said user enters said PIN number with at least one of said at least two digits used for said security segment.

This appeal arises from the Examiner's Final Rejection, mailed November 23, 2005. The Appellant filed a Brief in support of the appeal on April 26, 2006, and the Examiner mailed an Answer to the Appeal Brief on May 30, 2006. A Reply Brief was filed on August 3, 2006.

PRIOR ART

The prior art references of record relied upon by the Examiner in rejecting the appealed claims are:

Zingher	US 5,731,575	Mar. 24, 1998
Franklin	US 5,883,810	Mar. 16, 1999
Rogers	US 5,946,386	Aug. 31, 1999
Hoffman	US 6,366,682 B1	Apr. 2, 2002 (Oct. 30, 1998)

REJECTIONS[2]

Claims 1-7, 9, 42-45 and 61 stand rejected under 35 U.S.C. § 103(a) as obvious over Hoffman and Zingher.

Claims 10-17, 25-41, 46-60, 62-64 and 122 stand rejected under 35 U.S.C. § 103(a) as obvious over Hoffman, Zingher, and Rogers.

Claims 18-24 stand rejected under 35 U.S.C. § 103(a) as obvious over Hoffman, Zingher, Rogers, and Franklin.

---

[2] The Answer details the rejections as claims 1-7, 9-17, 35-36, 42-45, and 61 over Hoffman and Zingher; 25-34, 37-41, 46-60, 62-64 and 122 over Hoffman, Zingher, and Rogers; and 18-24 over Hoffman, Zingher, and Franklin. However, this characterization is technically inaccurate because claim 122, from which claims 10-41 depend, includes Rogers in its rejection. Both the Examiner's and the Appellant's arguments are consistent with the application of the art indicated above, in which all claims depending from claim 122 also include Rogers in their rejections, and so therefore, the rejections are treated as such.

The Examiner applies Zingher to show the use of Personal Identification Number (PIN) digits adapted for use to trigger an alarm for use under duress; Hoffman to show implementation details of PIN systems, Franklin for implementation details of purchase transactions that might use PIN's; and Rogers to show evidence that system centers that control PIN access would also have facilities such as e-mail, facsimile and paging communication.

ISSUES

The issues pertinent to this appeal are

Independent claims 1, 42, and 122 rejected under 35 U.S.C. § 103(a).

- Whether the art shows selecting at least two digits for a security segment to be incorporated into a PIN number wherein an alarm signal is sent when a user enters that PIN number with at least one of at least two digits used for the security segment
- Whether the art, and in particular, regarding claim 42, the combination of Zingher and Hoffman shows performing e-mail, voice messaging, and financial transactions
- Whether there is motivation in the prior art to combine the references

Dependent claims 2-7, 9-17, 21, 22, 35, 36, 43-54 and 61 rejected under 35 U.S.C. § 103(a).

- Whether the art shows or suggests use of a telephone number for a PIN
- Whether the art shows selecting a digit in said first segment to identify the location of said second security segment

- Whether the art shows entering both an identification and PIN number, the PIN either with or without the security segment, to receive money
- Whether the art shows inserting a credit card or identification card prior to entering the identification number (claim 14)
- Whether the art shows having the user specify an activation time, at least one monitoring location and at least one assistance preference and calling the user at that activation time at the monitoring location

Dependent claims 18-20, 23, and 24 rejected under 35 U.S.C. § 103(a).

- Whether the art shows downloading information stored in a buffer; opening a temporary file containing the downloaded information; assigning a transaction identification number to the temporary file; and transferring the transaction identification number to the buffer and verifying the transaction identification number

Dependent claims 25-34, 37-41, 46-60 and 62-64 rejected under 35 U.S.C. § 103(a).

- Whether the art shows providing an electronic box for providing at least one of an indication of the presence of an e-mail message, the names of the individual transmitting the e-mail message, and the text of the e-mail message
- Whether the art shows triggering a notification signal when said user uses a particular credit or debit card

In particular, the Appellant contends that the art does not show the two digits for a PIN security segment (Br. 21-23); that neither Hoffman nor Zingher shows performing e-mail, voice messaging and financial transactions (Br. 23-24); that

there is no motivation to combine Rogers's call center with Hoffman or Zingher (Br. 24-26); that the art fails to show use of a telephone number for a PIN (Br. 27); that the art fails to show selecting a digit in said first segment to identify the location of said second security segment (Br. 27); that the art fails to show entering both an identification and PIN number, the PIN either with or without the security segment, to receive money (Br. 27-29); that the art fails to show inserting a credit card or identification card prior to entering the identification card (claim 14); that the art fails to show having the user specify an activation time, at least one monitoring location and at least one assistance preference and calling the user at that activation time at the monitoring location (Br. 29-30); downloading information stored in a buffer; opening a temporary file containing the downloaded information; assigning a transaction identification number to the temporary file; and transferring the transaction identification number to the buffer and verifying the transaction identification number (Br. 30-32); there is no reason to apply Rogers's communications teachings to Hoffman (Br. 32-40); that the art fails to show providing an electronic box for providing at least one of an indication of the presence of an e-mail message, the names of the individual transmitting the e-mail message, and the text of the e-mail message (Br. 36); and that the art fails to show triggering a notification signal when said user uses a particular credit or debit card (Br. 37).

FACTS PERTINENT TO THE ISSUES

The following findings of fact (FF) pertinent to the issues in this appeal are supported by a preponderance of the evidence.

1) Each of the three independent claims, *viz.* 1, 42, and 122, call for a PIN that has two segments. One segment is comprised of a plurality of selected digits. The other segment is comprised of at least one digit, which, when entered within the PIN entry, triggers an alarm.

2) Claim 1 adds a further limitation that at least two digits are selected for the second segment, however, by the terms of claim 1, entry of at least one of them is sufficient to trigger the alarm.

3) Choosing a second digit that is not used is a nonfunctional statement of intended use relative to the operation of claim 1.

4) A PIN is an authentication code, or as Zingher refers to it (Zingher, col. 1, ll. 49-52), an access code.

5) A PIN authenticates, i.e., grants access to, the person whose identification, either by entry of an identification number, such as an account number, or its equivalent by biometric measurement, has been entered.

6) Entry of an identification number at an ATM or at a merchant's terminal is generally by a card identifying the user and the user's account.

7) Thus, use of a PIN inherently comprises entry of both an identification datum, such as a number, and the PIN. This is evidenced by the Background section of Hoffman (Hoffman, col. 1, ll. 45-60).

8) Zingher describes the use of multiple sets of digits that may be entered when a system is expecting a PIN to be entered. Zingher refers to a set of digits that are entered when PIN entry is expected, but is meant to trigger an alarm as a personal distress number (PDN) (Zingher, col. 2, l. 66- col. 3, l. 11).

9) Thus, each of the numbers characterized as PINs in independent claims 1, 42, and 122, is the functional equivalent of what Zingher refers to as a PDN when the claimed segment with claimed digit is entered that triggers an alarm.

10) Zingher describes several methods for devising a PDN. In particular, Zingher refers to methods involving an altered PIN, particularly

> (1) a typical prestored PIN number prestored in the memory banks of the bank computer or on the magnetic strip of the costumer's [sic] card, and (2) an algorithm which may alter the PIN number to achieve a PDN number.

(Zingher, col. 3, ll. 26-29).

In particular, Zingher describes implementations in which

> the PIN could be N digits in length and the PDN could be either N-1, N, or N+1 digits. By expanding the range of PIN lengths, the PDN length could also be shortened or lengthened as required. There is no requirement that the extra digit be specifically designated. That is, any digit in the N+1 position could be used to trigger the alarm system. All the customer has to know is to press any extra digit he wants to.

(Zingher, col. 11, ll. 39-46).

11) Thus, Zingher describes selecting any digit, which is one of at least two digits, for a security segment to be incorporated into a PIN number wherein an alarm signal is sent when a user enters that PIN number with at least one of at least two digits used for the security segment.

12) Similarly, Zingher suggests selecting a digit in said first segment (N) to identify the location of said second security segment (N+1).

13) Similarly, Zingher suggests entering both an identification and PIN number, the PIN either with (thus forming Zingher's PDN) or without (thus forming Zingher's PIN) the security segment, to receive money.

14) Similarly, the use of a credit card or a bank card at an ATM suggests inserting a credit card or identification card prior to entering a PIN, although nothing in the art of record suggests entering both the identification number and PIN after inserting such a card.

15) Rogers describes performing voice messaging, e-mail, Fax, and data messaging (col. 4, ll. 27-34). Hoffman, Zingher, and Franklin each describe financial transactions in their background. As to the combined teachings of Hoffman and Zingher, absent Franklin, in particular, Hoffman describes a terminal that

> communicates through a modem 18 with the DPC 1 through transaction request messages 19 and transaction response messages 20 using one of the interconnecting means in FIG. 1 such as a cable TV network, cellular telephone network, telephone network, the Internet, or an X.25 network.

(Hoffman, col. 9, ll. 38-43).

16) These transaction messages are commonly conveyed via voice messaging, e-mail, Fax, and data messaging.

17) Thus, Zingher and Hoffman in particular, and more generally, those references coupled with Rogers, show performing e-mail, voice messaging, and financial transactions.

18) Zingher suggests the use of the user's telephone numbers for a PIN or PDN (Zingher, col. 6, ll. 51-56).

19) Thus, Zingher suggests use of a telephone number for a PIN.

20) As the Examiner pointed out (Answer 6), Franklin describes the internal mechanics of using a credit or debit card with a PIN in a commercial transaction

where the issuing bank creates a temporary customer account record in the customer database 64 and assigns a temporary PIN (personal identification number) or other type of customer identifier to that account.

(Franklin, col. 6, ll. 50-54).

Of greater pertinence, Franklin later describes, in thorough detail, numerous instances of downloading information stored in a buffer; opening a temporary file containing the downloaded information; assigning a transaction identification number to the temporary file; and transferring the transaction identification number to the buffer and verifying the transaction identification number in

> the online commerce system 20 during a transaction phase. This phase involves the customer 22 engaging in an online commerce transaction with the merchant 24. As part of the process, the customer 22 requests a transaction number from the bank 26 to be used in the commerce transaction. . . .
>
> Upon reaching this method of payment field, the customer clicks the card button UI 54 on the browser toolbar to invoke a card transaction module 72. . . .
>
> Upon clicking the button UI 54, a dialog box appears on the display to inform the customer that they have requested a secure card number. The customer is prompted by the dialog box to input a password for identification purposes. This password might be the private key (if the customer knows the key value) or it may be a separate name or number created by the customer. The operating system 48 checks the password prior to allowing access to the certificate store 50. If the password is approved, the transaction module 72 prepares a request for a transaction number, digitally signs the request using the customer's private key, and submits the signed request to the issuing bank's computer 32 via the Internet 34 (flow arrow 2 in FIG. 3). The request contains the certificate originally issued by the bank.
>
> . . . Assuming the signature and request are valid and the customer's account is in good standing, the account manager 60 instructs the

transaction number generator 62 to create a transaction number to be used as a proxy for the customer account number during the online commerce transaction. The account manager 60 associates the transaction number with the customer account number in a data record on the customer database 64. As a result, the online commerce card now has two numbers associated therewith: a permanent customer account number and a transaction number that serves as a proxy for the customer account number.

FIG. 4 shows one exemplary implementation of creating a transaction number and associating that number with the customer's account number. A customer record 80 for the requesting customer is stored in the customer database 64 and contains a customer account number. Suppose, for example, the customer account number is a 16-digit credit card number. Credit card numbers comply with a standardized format having four spaced sets of numbers, as represented by the number "0000 0000 0000 0000". The first five-to-seven digits are reserved for processing purposes. It identifies the issuing bank, the card type, and so forth. The last 16th digit is used as a sum check for the 16-digit number. The intermediary eight-to-ten digits are used to uniquely identify the customer.

The transaction number generator 62 generates a transaction number for the online commerce card that is formatted identically to the customer account number. In this example, the number generator 62 creates a 16-digit transaction number having four spaced sets of numbers, as represented by the number "1111 1111 1111 1111". The transaction number resembles a credit card number in all respects, except that the first five-seven-digits are coded by the issuing bank to identify the number as a fictitious electronic proxy number, rather than a real credit card number.

The account manager 60 associates the temporary transaction number with the permanent customer account number by relating the two numbers in a data record 82. More particularly, the account manager creates data record 82 in a proxy/customer account cross-reference database. The data record 82 is keyed with the customer account number to identify the customer record 80. The transaction number is then written to the data record 82. In this manner, the customer account record 80 can be cross-referenced via the

transaction record 82 using the transaction number as an index. The issuing bank will use the transaction record 82 at a later time when the merchant submits the transaction number for payment authorization.

. . . The transaction number is valid for only one transaction. For added security, the transaction number can be linked to transaction information to ensure that the number is only used for one specific transaction. The transaction module 72 executing on the customer computer 28 may require the customer to enter information pertaining to the purchase, like the purchase price, the model or item number, the merchant name, and the like. The issuing bank can then tie the transaction number to this specific transaction data within the transaction record 82.

Once the transaction record 82 is created and related to the customer record 80, the issuing bank computer 32 sends the transaction number to the customer computer 28 (flow arrow 3 in FIG. 3). The real customer account number is not sent to the customer, but is retained at the issuing bank in secrecy. In the credit card case, this means that the true credit card number is never sent over the Internet 34, thereby eliminating the possibility of interception and illicit use by a thief.

At the customer computer, the transaction number is presented in a graphical window by the transaction module 72. If the order form is compatible, the customer can click on an icon to have the number automatically entered into the merchant order form 70. Otherwise, in a worst case scenario, the customer manually enters the proxy transaction number into the merchant's HTML order form 70. Since the transaction number has the identical 16-digit format as a real credit card number, the customer enters the 16-digit number as if it were his/her real credit card number.

The user may also be required to enter an expiration date, which may or may not be sent from the issuing bank. Essentially, the expiration date can be any future date that is not too far in the distant future, such as less than two to three years. The customer then submits the completed order form 70 over the Internet 34 to the merchant computer 30.

Authorization Phase

FIG. 5 shows the online commerce system 20 during a payment authorization phase. This phase involves the merchant 24 seeking authorization from the issuing bank 26 to honor the customer's transaction number received by the merchant in the commerce transaction with the customer. The information exchange between the merchant computer 30 and the bank computer 32 during the authorization phase are illustrated as enumerated lines.

The merchant 30 receives the transaction number from the Internet and processes the transaction number using its existing computer system. There is no software components added to the merchant computer as part of the online commerce system 20. Rather, the merchant computer 30 treats the transaction number of the online commerce card no differently than it treats a standard credit card number. In fact, the merchant computer 30 most likely will not be able to distinguish between the two types of numbers.

In FIG. 5, the merchant computer submits a request for authorization over a payment network 36 to the bank computing center 32 (flow arrow 1 in FIG. 5). This illustration is simplified for discussion purposes, as other participants will most likely be involved. For instance, the merchant computer 30 typically submits the request for authorization to its acquiring bank (not shown) by conventional means. The acquiring bank validates the authorization request by verifying that the merchant is a valid merchant and that the credit card number represents a valid number. The acquiring bank then forwards the authorization request to the issuing bank. The routing to the issuing bank via the payment network is handled through conventional techniques.

When the bank computer 32 receives the authorization request, it first examines the transaction number to determine whether it is a valid number. A transaction number identifier 90 executing at the bank computer 32 examines all incoming account numbers to segregate proxy transaction numbers from real credit card numbers. On a daily basis, it is likely for the bank computer 32 to handle many account numbers on the order of tens or hundreds of thousands. Most of the numbers are expected to be real credit card account numbers. Only a small percentage is anticipated to be temporary transaction numbers. The transaction number identifier 90 filters out authorization

> requests that pertain to transaction numbers from authorization request that pertain to real customer account numbers. In the continuing example, the transaction number identifier 90 recognizes the number submitted by the merchant computer 30 as a transaction number based on the first five-to-seven digits.
>
> The transaction number identifier 90 passes the transaction number to the account manager 60. The account manager 60 uses the transaction number as an index to transaction records in the customer database 64. If no records are found, the number is deemed invalid and the bank computer 32 returns a message disapproving the transaction to the merchant computer 30. If a record is found, the account manager 60 examines any extra transaction information, such as purchase amount and merchant ID, which is typically included in the authorization request to double check the accuracy of the request.
>
> Once a valid transaction record 82 is located, the account manager 60 cross-references to the associated customer account number and uses this number to index the customer record 80. The account manager 60 substitutes the customer account number in place of the transaction number in the merchant authorization request. The account manager 60 then submits the authorization request to the bank's traditional processing system 92 for normal authorization processing (e.g., confirm account status, credit rating, credit line, etc.).
>
> After the request is processed, the processing system 92 returns an authorization response to the account manager 60. The account manager fetches the transaction number from the cross-referenced data records 80 and 82 in the database 64 and substitutes the transaction number in place of the customer account number in the bank's authorization reply. The bank computing center 32 then returns the authorization reply to the merchant computer 30 via the payment network 36 (flow arrow 2 in FIG. 5).

(Franklin, col. 8, l. 15 – col. 11, l. 40).

Similarly, Hoffman describes an internet point of sale terminal (IPT), in which

> [i]n addition to identifying the buyer, the IPT must also identify the remote seller who is the counterparty to the transaction. The seller must also identify both the DPC [data processing center] and the IPT.

> The Internet Shopper program stores the hostname (or other form of net name) of the seller from which the purchase is taking place so that the DPC can verify the seller's identity. . . .
>
> First, the IPT connects to the seller using the Internet. . . .
>
> Once connected, the IPT downloads the seller identification code, and both price and product information from the seller. Once the buyer is ready to make a purchase, he selects the merchandise he wishes to buy. Then, the buyer enters the biometric-PIN using the BIA/PC [biometric input apparatus / personal computer], the IPT sends the seller identification code, the product identification information, and the amount to the BIA, and instructs it to construct a Remote Commercial Transaction Message. Then the IPT sends the request to the seller via the secure channel.
>
> . . . The DPC validates the biometric-PIN, cross-checks the seller identification code contained in the request with the seller identification code stored under the hostname that was sent in the request, and then sends a transaction to the credit/debit network. Once the credit/debit network responds, the DPC constructs a response message including the credit/debit authorization, an encrypted private code, and the address of the buyer, and sends that message back to the seller.
>
> Once the seller receives the response, it copies the buyer's mailing address out of the response, makes note of the authorization code, and forwards the response message to the IPT.

(Hoffman, col. 15, l. 44 – col. 16, l. 27).

21) Thus both Franklin and Hoffman describe the act of creating a temporary record including downloaded purchaser identification and PIN and seller identification information stored in a buffer; opening a temporary file containing the downloaded information; assigning a transaction identification number to the temporary file; and transferring the transaction identification number to the buffer and verifying the transaction identification number to create a Remote Commercial Transaction Message.

22) Rogers describes providing an electronic box in fig. 6c for providing all of, and therefore at least one of, an indication of the presence of an e-mail message, the names of the individual transmitting the e-mail message, and the text of the e-mail message.

23) Credit card issuers have triggered notification signals in the form of monthly statements since the inception of credit cards. The notification signal of each use was added to the database for the monthly billings whenever a particular credit card was used. On-line banking software, suggested by the on-line commerce transactions of Franklin, are notoriously old and well known to have triggered an electronic notification signal whenever a user used a particular credit or debit card since at least as far back as the introduction of Quicken 98 in 1998.

24) Zingher provides implementation details for securing the PIN taught by Hoffman.

25) Franklin provides implementation details for how the transactions described by Hoffman are executed.

26) Rogers provides an exemplary environment in which Zingher's security over PINs may be needed with Rogers's security code (Rogers, col. 44, ll. 1-4). Rogers also describes its call center operations as a mechanism for handling business communications (Rogers, col. 1, ll. 42-47).

27) Both Franklin and Hoffman describe financial transactions that are conveyed via the conduits of business communications, which Rogers provides more efficient and effective operations over.

28) Thus, it would have been obvious to a person of ordinary skill in the art to have applied the teachings of Zingher and Franklin to Hoffman to find

implementation details and to have applied Rogers to Hoffman for greater efficiency in Hoffman's operations.

ANALYSIS

Claims 1-7, 9, 42-45 and 61 rejected under 35 U.S.C. § 103(a) as obvious over Hoffman and Zingher

and

Claims 10-17, 25-41, 46-60, 62-64 and 122 rejected under 35 U.S.C. § 103(a) as obvious over Hoffman, Zingher, and Rogers.

The above findings of fact demonstrate that

- The art shows selecting at least two digits for a security segment to be incorporated into a PIN number wherein an alarm signal is sent when a user enters that PIN number with at least one of at least two digits used for the security segment (FF 11).
- The art, and in particular, regarding claim 42, the combination of Zingher and Hoffman, coupled with Rogers, shows performing e-mail, voice messaging and financial transactions (FF 17).
- It would have been obvious to a person of ordinary skill in the art to have applied the teachings of Zingher to Hoffman to find implementation details and to have applied Rogers to Hoffman for greater efficiency in Hoffman's operations (FF 28).
- The art shows or suggests use of telephone number for a PIN (FF 19).
- The art shows selecting a digit in said first segment to identify the location of said second security segment (FF 12)

- The art shows entering both an identification and PIN number, the PIN either with or without the security segment, to receive money (FF13)
- The art shows inserting a credit card or identification card prior to entering a PIN, but not prior to entering both the identification number and PIN (claim 14) (FF 14).

Further, the art does not show having the user specify an activation time, at least one monitoring location, and at least one assistance preference and calling the user at that activation time at the monitoring location of claims 35 and 36, nor has the Examiner pointed to anywhere in the art of record that this subject matter is described.

Thus, the Examiner has shown by a preponderance of substantial evidence that the claim limitations of claims 1-7, 9-13, 15-17, 25-34, 37-64 and 122 are found in or suggested by the art and that it would have been obvious to a person of ordinary skill in the art to have combined the respective teachings. Accordingly we sustain the Examiner's rejection of claims 1-7, 9, 42-45 and 61 under 35 U.S.C. § 103(a) as obvious over Hoffman and Zingher and we sustain the Examiner's rejection of claims 10-13, 15-17, 25-34, 37-41, 46-60, 62-64 and 122, but do not sustain the rejection of claims 14, 35, and 36, under 35 U.S.C. § 103(a) as obvious over Hoffman, Zingher, and Rogers.

Claims 18-24 rejected under 35 U.S.C. § 103(a) as obvious over Hoffman, Zingher, Rogers, and Franklin.

The above findings of fact demonstrate that

- The art shows downloading information stored in a buffer; opening a temporary file containing the downloaded information; assigning a transaction identification number to the temporary file; and transferring the transaction identification number to the buffer and verifying the transaction identification number (FF 21).
- The art shows providing an electronic box for providing at least one of an indication of the presence of an e-mail message, the names of the individual transmitting the e-mail message, and the text of the e-mail message (FF 22).
- The art shows triggering a notification signal when said user uses a particular credit or debit card (FF 23).
- It would have been obvious to a person of ordinary skill in the art to have applied the teachings of Zingher and Franklin to Hoffman to find implementation details and to have applied Rogers to Hoffman for greater efficiency in Hoffman's operations (FF 28).

The Appellant argued that the Examiner improperly rejected claims 21 and 22 on the technical basis that their rejection did not include the same art as their parent claim 20 (Br. 29), which the Examiner noted and corrected (Answer 2-3). The Appellant did not recite any argument in the Reply Brief regarding patentability of claim 21 and 22, but only commented that they did not see the Examiner pointing out the analysis for their patentability (Reply Br. 5-6). Our reviewing court has recently held that, while it is correct that each claim must be considered separately, where the dispositive issue, in this case using a PIN with a security segment and a transaction identifier in a transaction, has been considered, and its analysis set forth

elsewhere in the opinion, failure to set forth this analysis separately for each affected claim on a claim by claim basis does not represent reversible error. *Hakim v Cannon Avent Group,* No. 2005-1398, slip op. (Fed. Cir., Feb. 23, 2007). Certainly the limitations added by claims 21 and 22 of debiting and crediting accounts for purchases have been inherent to purchases for a notoriously old duration, essentially having existed at least since Luca Pacioli first codified double entry accounting in 1494, and are therefore of minimal weight in terms of patentability analysis.

Thus, the Examiner has shown by a preponderance of substantial evidence that the claim limitations of claims 18-24 are found in or suggested by the art and that it would have been obvious to a person of ordinary skill in the art to have combined the respective teachings. Accordingly we sustain the Examiner's rejection of claims 18-24 under 35 U.S.C. § 103(a) as obvious over Hoffman, Zingher, Rogers and Franklin.

DECISION

To summarize, our decision is as follows:

- The rejection of claims 1-7, 9, 42-45 and 61 under 35 U.S.C. § 103(a) as obvious over Hoffman and Zingher is *sustained.*
- The rejection of claims 10-13, 15-17, 25-41, 46-60, 62-64 and 122 under 35 U.S.C. § 103(a) as obvious over Hoffman, Zingher, and Rogers is *sustained.*
- The rejection of claims 14, 35-36 under 35 U.S.C. § 103(a) as obvious over Hoffman, Zingher, and Rogers is *not sustained.*

- The rejection of claims 18-24 under 35 U.S.C. § 103(a) as obvious over Hoffman, Zingher, Rogers, and Franklin is *sustained.*

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a) (2006).

AFFIRMED-IN-PART

hh

Barry L Kelmachter
Bachman & LaPointe PC
Suite 1201
900 Chapel Street
New Haven, CT 06510-2802